**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, Plaintiff, —*against*— CITIBANK, N.A., Defendant.	24 Civ. 0659 (JPO)

**CITIBANK, N.A.'S MEMORANDUM OF LAW
IN SUPPORT OF ITS MOTION TO DISMISS**

STEPTOE LLP
1114 Avenue of the Americas
New York, New York 10036
(212) 506-3900

2029 Century Park East
Suite 1800
Los Angeles, CA 90067
(213) 439 9400

April 2, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

REGULATIONS

ADMINISTRATIVE MATERIALS

LEGISLATIVE HISTORY MATERIALS

TREATISES

OTHER AUTHORITIES

INTRODUCTION

This case is a misguided attempt by the New York Attorney General's Office ("NYAG") to circumvent Congress and rewrite the federal Electronic Fund Transfer Act of 1978 (the "EFTA") to provide consumer relief that NYAG apparently wishes had been included by Congress, but quite plainly was not. Over the decades since the EFTA became law, no one has suggested that the EFTA means what NYAG is now claiming. The proper forum for pursuing the goals NYAG seeks to achieve in this litigation is in Congress, not a courtroom.

The backdrop for this case is the problem of online wire fraud. There is no denying that the problem is real. Scammers have found increasingly sophisticated ways to fraudulently wire themselves money from consumers' bank accounts. Defendant Citibank, N.A. ("Citibank") takes this problem seriously, and has implemented robust countermeasures. But no system will catch every scam every time. That is especially true in the circumstances alleged here, where NYAG describes consumers who fell for "phishing" scams or otherwise provided security information, such as codes texted from Citibank, directly to scammers.

The core issue raised by this case is the scope of Citibank's responsibility to reimburse consumers who fall victim to wire fraud scams. The answer lies in Article 4A of the Uniform Commercial Code ("UCC"), which governs wire transfers. Generally speaking, a bank that follows a commercially reasonable "security procedure" in good faith to verify a customer's identity will not be responsible for the customer's loss. The banking industry and courts have for decades applied Article 4A to wires, including consumer wires, and the industry has developed systems and procedures based on Article 4A's terms.

NYAG's Complaint is premised on the novel theory that Citibank and the rest of the industry have been applying the wrong legal framework all this time. According to NYAG, consumer wires should be governed by the separate legal framework of the EFTA, which

governs electronically-initiated fund transfers by consumers, such as ATM transactions. Under the EFTA, a consumer's exposure for fraudulent fund transfers (*e.g.*, a stolen ATM card) is typically capped at $50. Just as banks have organized their wire businesses around Article 4A, banks have developed systems and procedures for EFTA-governed transactions based on a settled understanding of where the EFTA applies and where it does not. That is why, for example, there are typically daily withdrawal limits at ATMs.

The two legal frameworks—the EFTA and Article 4A—are intended to be mutually exclusive, reflecting careful judgment by Congress and state legislatures that the wire systems, which typically involve large-dollar business transfers, should be governed by rules that promote efficiency and finality, while still providing important protections to users. The careful delineation of these two legal regimes is reflected in the EFTA's ***express exclusion of wire transfers*** from its coverage; in contrast, wire transfers are the principal focus of Article 4A. Decades of regulatory enactments and guidance further confirm that wire transfers, including consumer wire transfers like those at issue here, are governed by Article 4A and ***not*** the EFTA.

Attempting to overcome the plain language of the EFTA's wire exemption, NYAG proposes to artificially separate the interdependent steps in a wire transfer so that only one part (the "bank-to-bank" transmission) is considered the EFTA-exempted wire, while another (the sending bank debiting its customer) is a freestanding, non-wire transaction governed by the EFTA. This imaginative theory is fundamentally flawed because the wire exemption refers specifically to wires initiated by "consumers" and so cannot be limited, as NYAG theorizes, to the "bank-to-bank" component. NYAG's approach deletes the "consumer" from the statutory text. NYAG's reading has the related problem of rendering the wire exemption meaningless. If a wire transfer is narrowly conceived as only a transmittal between banks, there would be no

reason for Congress to have exempted those transactions from the EFTA, which as enacted by Congress only reaches consumer transactions.

NYAG's theory not only mangles the EFTA's text, but defies longstanding, settled understandings of the EFTA in the banking industry. Over the decades, there is every indication—from regulators, academics and even consumer advocates—that the EFTA applies as the industry has understood it, and ***zero*** evidence of NYAG's interpretation. In fact, this widespread understanding is why Congress recently considered a bill titled "Protecting Consumers From Payment Scams Act," which would delete the wire exemption. The bill failed to pass. The Court should approach with great skepticism NYAG's novel interpretation, one which has somehow managed to elude lawmakers, regulators, courts and the industry for so long, and which would bring about—via litigation, not legislation—a sea change in banking law.

NYAG's Complaint asserts eight causes of action, in each instance invoking New York's prohibition in the Executive Law against "engag[ing] in repeated fraudulent or illegal acts." N.Y. Exec. L. § 63(12). All eight fail to allege illegality or fraud, and should be dismissed, as demonstrated below.

EFTA: Reimbursement (First Cause of Action). NYAG alleges that Citibank fails to apply the EFTA for fraudulent consumer wires, but, as discussed, the EFTA exempts wires altogether and is inapplicable.

EFTA: Transfers Between Customer's Accounts (Second Cause of Action). NYAG argues that Citibank should be held liable for unauthorized transfers between a single customer's own accounts (such as from savings to checking), but in those instances the transfer does not meet the statutory definition of an "unauthorized" transfer and, regardless, there is no loss for NYAG to recover.

EFTA: Disclosures and "Illegal" Agreements (Third Cause of Action). NYAG argues that banks are required to disclose in "clear terms" the specific security procedures employed to combat fraud, notwithstanding that the EFTA nowhere calls for banks to provide a roadmap for scammers in this way (nor should it). NYAG also alleges that Citibank's customer agreements violate the EFTA's provision against contractual waivers of its terms, but NYAG misconstrues the EFTA's requirements and Citibank's agreements.

UCC Article 4A (Fourth Cause of Action). NYAG alleges, in the alternative, that Citibank does not employ commercially reasonable security procedures under Article 4A, but fails to set forth sufficient facts to state a claim. Although the Complaint recounts how ten Citibank consumers were allegedly victimized by scammers, NYAG fails to plead critical facts concerning the procedures Citibank employed to verify those wires, creating the false impression that these instances where sophisticated scammers happened to succeed reflect the norm. They do not. NYAG's inadequately-pleaded claim must be dismissed.

SHIELD Act (Fifth Cause of Action). The Complaint likewise fails to state a claim that Citibank violated New York's "SHIELD Act"—an anti-hacking statute obligating covered businesses to adopt procedures to prevent, and give notice of, data breaches. This case is not about anyone hacking into Citibank's systems. To the contrary, as the Complaint concedes, the scammers obtained customers' data either by tricking them or, in one instance, from another company's data breach. To the extent NYAG misreads the statute to sweep in the wire fraud scenarios alleged, the claim is preempted by the Fair Credit Reporting Act ("FCRA").

Red Flags Rule (Sixth Cause of Action). Citibank's alleged violation of the federal identity theft prevention regulation known as the "Red Flags Rule," adopted under the FCRA, similarly should be dismissed because NYAG's attempt to enforce the rule is preempted by the

FCRA. Even if not preempted, the claim is meritless. The Red Flags Rule requires banks to implement programs "designed to detect, prevent, and mitigate identity theft," but NYAG does not allege (nor could it credibly allege) that Citibank lacks the required programs.

Fraud and Consumer Deception (Seventh and Eight Causes of Action). NYAG's accusations of fraud and deception are premised on generic advertising statements, such as "your security is important to us," and the allegation that Citibank's procedures for handling fraud complaints are different from what NYAG would prefer. None of these statements or procedures amount to actionable fraud or deception.

* * *

Citibank devotes substantial resources to combatting online fraud and to protecting its customers, and will continue to do so. Citibank's significant anti-fraud practices have stopped countless fraudulent transactions and protect consumers from scammers every day. The solution to the problem of online wire fraud and scams is not a lawsuit, especially one that improperly seeks to rewrite a federal statute and that would abruptly and dramatically upset how banks have organized their policies and practices for decades.

The Complaint should be dismissed in its entirety.

BACKGROUND

A. The Statutory Framework for Consumer Wire Transfers

1. The EFTA and Its Wire Exemption

In November 1978, Congress passed the EFTA. Pub. L. 95-630 § 2001 (1978). The law was intended to address certain "relatively new banking and payment services" that used "computer and electronic technology" instead of paper, such as ATMs and electronic terminals that allowed consumers to pay for goods at a store. S. Rep. No. 95-915, at 2-3 (1978). The bill followed the "key recommendation" of a Congressionally-commissioned report from the

National Commission on Electronic Fund Transfers ("NCEFT"), *see* Pub. L. 93-495 §§ 201-08 (1974), to establish an "EFT Bill of Rights" for consumers using those new services. S. Rep. No. 95-915, at 3 (citing NCEFT, *EFT in the United States, Policy Recommendation and the Public Interest* (Oct. 28, 1977) ("NCEFT Report")) (Ex. A).[1] Congress sought to grant consumers statutory rights governing unauthorized or errant transactions, and to mandate certain disclosures about account terms and transactions. S. Rep. No. 95-915, at 3-8.

As enacted, the EFTA applies to any "electronic fund transfer," which is defined as a transfer of funds "initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account," subject to specified exemptions. 15 U.S.C. § 1693a(7). The term "account" is defined, in turn, as one "established primarily for personal, family, or household purposes." *Id.* § 1693a(2). Among other things, the EFTA provides that consumers who promptly give notice of an unauthorized transfer are generally responsible only for the first $50 of losses. *Id*. § 1693g(a).

Most relevant here, the EFTA has since its passage expressly excluded from its coverage any transfer "on behalf of a consumer by means of a service that transfers funds held at either Federal Reserve banks or other depository institutions and which is not designed primarily to transfer funds on behalf of a consumer." Pub. L. 95-630 § 2001 (1978) (codified at 15 U.S.C. §1693a(7)(B)). Although the "service[s]" are not identified by name, Congress was referring to wire services like Fedwire (operated by the Federal Reserve) and CHIPS (operated by private banks). Regulations and guidance have since made that clear.[2]

[1] Citations in the form Ex. __ refer to the exhibits to the accompanying Declaration of Charles Michael. The NCEFT report and other legislative history materials are properly the subject of judicial notice and may be considered on a motion to dismiss. *Goe v. Zucker*, 43 F.4th 19, 29 (2d Cir. 2022) (holding that "courts may take judicial notice of legislative history" and other administrative materials, and doing so in connection with a motion to dismiss).

[2] *See* 12 C.F.R. § 1005.3(c)(3); Electronic Fund Transfers, 61 Fed. Reg. 19,662, at 19,663 (May 2, 1996).

2. Congress Chose Not to Include Wires in the EFTA's Scope

The legislative history of the wire exemption confirms that Congress made a deliberate choice. The NCEFT Report that laid the foundation for the law focused its recommendations on the "new" electronic transfer systems, such as ATMs and payment terminals. NCEFT Report, at 1-2. Although the report acknowledged the two major wire systems that still dominate the U.S. Dollar domestic market today—Fedwire and CHIPS—and noted that Fedwire had been in operation since 1918, *id.* at 338-39, the Report made ***no recommendations*** for any regulation of those systems. That omission is all the more notable because the Report observed that there were instances where consumers could use Fedwire: "consumers may send funds on the Federal Reserve wire network by using the facilities of a member bank." *Id*. at 338.

Even beyond the NCEFT Report, the existence of consumer wires—and the possibility of including them in the new law—was squarely before Congress. On at least three occasions, hearing witnesses urged Congress to apply the new law to consumer wires:

- A Harvard professor told the Senate Banking Committee that there should be a "consistent set of principles applicable" to all payment systems, including wire transfers, and asked why the bill should "leave entirely uncovered . . . bankwire" transactions. *See Consumer Protection Aspects of EFT Systems, Hearings on S. 3546, S. 2470*, 95th Cong. 75-76, 79, 82 (1978). (Ex. B.)[3]

- The President of a payment system called TYME (Take Your Money Everywhere), similarly urged Congress to ensure the bill would "encompass all facets" of electronic payment systems, including "automated bill paying services, ***wire transfer services***, etc.," because, in his view, the rights of consumers should be the same regardless of which of those means the consumer chooses, or even if the consumer uses "some as yet uninvented means." *See The Consumer Credit Protection Act Amendments of 1977, Hearings on H.R. 8753, Part 3*, 95th Cong. 1404, 1406 (1977) (emphasis added). (Ex. C.)

- The President of the Virginia Citizens Consumer Council, a "grass roots consumer organization" that served as a "nationwide clearing house for consumer comment and problems with electronic funds transfer," testified to the House

[3] Congressional hearing materials are "public records," which "courts in this District have found to be subject to judicial notice." *In re Moody's Corp. Sec. Litig.*, 599 F. Supp. 2d 493, 504 (S.D.N.Y. 2009).

> Banking Committee about an "attempt to steal $2 million dollars via a bogus wire," and warned that, since similar scams could impact a "large number of consumer accounts," Congress should apply to wires the same protections contemplated for "lost or stolen [debit] cards." *See The Consumer Credit Protection Act Amendments of 1977, Hearings on H.R. 8753, Part 1*, 95th Cong. 58, 62 (1977). (Ex. D.)

Yet, Congress did not take that approach. Congress chose ***not*** to regulate wire transfers—even though they "might otherwise be considered electronic fund transfers"—because they were not among the new technologies that "motivated passage" of the new law, and because wire transfers were "already governed by rules established by the Federal Reserve." Roland E. Brandel & Eustace A. Olliff III, *The Electronic Fund Transfer Act: A Primer*, 40 Ohio St. L. J. 531, 543-44 (1979). The Senate Report confirms that the EFTA was focused upon the "relatively new" consumer services that were "initiated and carried out primarily by electronic means," such as (1) ATMs and (2) "point-of-sale systems," where consumers could pay for goods at in-store terminals. S. Rep. No. 95-915, at 2-3 (1978). In short, Congress determined that wire transfers—whose technology and rules had been in place for decades—should be left undisturbed.

3. Regulation E and Subsequent Guidance Relating to the Consumer Wire Exemption

In 1979, the Board of Governors of the Federal Reserve System adopted "Regulation E" to implement the EFTA. *See* Electronic Fund Transfers, 44 Fed. Reg. 18,468 (Mar. 28, 1979); Electronic Fund Transfers, 44 Fed. Reg. 59,464 (Oct. 15, 1979). Regulation E's consumer wire transfer exemption largely tracked the statutory language, carving out "[a]ny wire transfer of funds ***for a consumer*** through . . . [a] network that is used primarily for transfers between financial institutions or between businesses." 44 Fed. Reg. 18,468, at 18,481 (emphasis added). As with the statutory language, the reference to a transfer "for a consumer" plainly contemplated (1) that consumers would be initiating wires and (2) that their wires would fall outside the EFTA.

Two years later, in 1981, the Federal Reserve issued Official Guidance as to Regulation E. Confirming that consumer wire transfers are viewed as ***including*** the sending or receiving consumer—not just the intermediate bank-to-bank component—the Guidance described the wire exemption as being triggered for a wire transfer with "instructions for crediting individual consumers' accounts":

> *3-2 Q: Wire transfer-instructions on magnetic tape*. If a transfer of funds to a financial institution is sent by Fedwire or a similar network, and the instructions for crediting individual consumers' accounts are transmitted on magnetic tape, are the transfers exempt?
>
> A: Yes. A Fedwire or similar transfer of funds is exempt.

Electronic Fund Transfers, 46 Fed. Reg. 46,876, at 46,879 (Sept. 23, 1981) (Question 3-2).

4. UCC Article 4A

In 1989, nine years after the EFTA's enactment, the National Conference of Commissioners on Uniform State Laws and the American Law Institute approved a new Article 4A of the Uniform Commercial Code. Its stated purpose was to provide a "comprehensive body of law that defines the rights and obligations that arise from wire transfers." *See* Uniform Laws Annotated, U.C.C. Article 4A, Prefatory Note (1989). UCC Article 4A broadly covers any transaction via a "payment order" to pay a beneficiary; in practice, this means payments "commonly referred to as wire transfers." N.Y. U.C.C. § 4-A-104(1) & Official Comment 6.

Generally speaking, wire transfers involve the exchange of payment messages among banks that settle with one another either periodically (*e.g*., at the end of the day) or in real time, and that settle their internal balances with their customers (the payor and payee) by crediting and debiting their accounts. 1 Benjamin Geva, *The Law of Electronic Funds Transfers* § 1.03 (2023).

The real-world nature and usage of wires "influenced the drafting of the statute," including that wires typically "involve[] a large amount of money," and are intended to be

completed in a single day, at low cost. *See* Uniform Laws Annotated, U.C.C. Article 4A, Prefatory Note (1989). Even when Article 4A was published in 1989, more than “one trillion dollars per day” passed through the wire systems. *Id*. The drafters of Article 4A understood that if these essential features of speed, efficiency and volume were to be preserved, banks could not be “exposed to very large liabilities in connection” with each wire. *Id*.

New York adopted Article 4A in 1990. *See* 1990 N.Y. Sess. Law Serv. 208. The New York Court of Appeals echoed the authors’ commentary in noting that Article 4A’s key goals were to ensure the “speed, efficiency, certainty . . . [and] finality” of wire transactions. *Banque Worms v. BankAmerica Int’l*, 570 N.E.2d 189, 195 (N.Y. 1991).

Transactions covered by the EFTA are expressly exempted from Article 4A because the drafters intended “to make Article 4A and EFTA mutually exclusive.” N.Y. U.C.C. § 4-A-108 & Official Comment. Accordingly, shortly after Article 4A was published, industry experts acknowledged that consumer wire transactions—by virtue of the EFTA’s wire transfer exemption—would be governed by the new Article 4A.[4]

The Federal Reserve saw this clear statutory interplay the same way. After Article 4A was released, the Federal Reserve overhauled the regulation governing Fedwire, Regulation J, to

[4] *See*, *e.g*., Carl Felsenfeld, *Strange Bedfellows for Electronic Funds Transfers: Proposed Article 4A of the Uniform Commercial Code and the UNCITRAL Model Law*, 42 Ala. L. Rev. 723, 736 (1991) (explaining that if “Mary in New York orders her bank to take $100 from her personal account and wire it to John in San Francisco,” and if the transaction were effectuated by wire, “it would be excluded from EFTA and thereby made subject to 4A”); Donald J. Rapson, *Outline of Highlights Article 4A – Funds Transfers*, C664 ALI-ABA 21, at *23 (Sept. 12, 1991) (Article 4A covers “all transactions, including consumer, using Fedwire, CHIPS and SWIFT”); Thomas C. Baxter, Jr. & Raj Bhala, *The Interrelationship of Article 4A With Other Law*, 45 Bus. Law. 1485, 1492 (1990) (“The analysis of a FedWire or CHIPS transaction is much easier. The presence of a consumer in funds transfers effected over these systems has no effect on the applicability of Article 4A because transfers over these systems are not ‘electronic funds transfers’ for purposes of the EFT Act. Consequently, all FedWire and CHIPS transfers are covered by Article 4A.”); Tomme Jeanne Fent, *Commercial Law: Electronic Funds Transfers: How New U.C.C. Article 4A May Affect Consumers*, 43 Okla. L. Rev. 339, 342 (1990) (“[C]onsumers who make wire transfers that are exempt from the EFTA may be subject to article 4A’s commercial rules.”); New Jersey Law Revision Commission, *Report and Recommendation Concerning Uniform Commercial Code Article 4A*, at 6 (Oct. 1990) (“Since, for practical purposes, any funds transfer that involves more than one bank is executed through a wire transfer system, any consumer transaction that is not executed within one bank is likely to be governed by Article 4A.”) (Ex. E).

apply Article 4A to all Fedwire transactions, even in states that had yet to adopt it. *See* Funds Transfers Through Fedwire, 55 Fed. Reg. 40,791, at 40,792 (Oct. 5, 1990). As with Article 4A, the revised Regulation J was intended to be mutually exclusive with the EFTA. *Id*. at 40,804. Accordingly, the Federal Reserve noted in its adopting release that Regulation J and Article 4A would govern a wire where the "originator's or beneficiary's account [was] a consumer account" because the EFTA and Regulation E "do not apply to funds transfers through Fedwire." *Id*.

Most relevant to this case, Article 4A addresses unauthorized transactions differently than the EFTA's near strict-liability regime. Generally, under Article 4A, banks are ***not*** responsible for unauthorized wire transfers if they follow commercially reasonable security procedures in determining whether the wires are authorized. N.Y. U.C.C. §§ 4-A-202(2), 4-A-204(1).

5. Congressional Efforts to Close the Consumer Wire Exemption

Wire services have become more commonly used by consumers (*e.g*., via smart phone apps) in recent years, leading to (unsuccessful) efforts before Congress to eliminate the EFTA's recognized consumer wire transfer exemption so that consumer wires would shift from the Article 4A framework to the EFTA. To date, however, Congress has not done so.

In April 2022, the House Financial Services Committee considered a bill entitled "Protecting Consumers From Payment Scams Act," which was intended to "eliminate EFTA's exemption for bank wire transfers." *See* H.R. Rep. No. 117-701, at 158 (2023); Protecting Consumers From Payment Scams Act § 2, 117th Cong., 2d Sess. (Ex. F). Notably, the National Consumer Law Center, a prominent consumer advocacy group, supported the amendment, acknowledging that "wire transfers are exempt from the EFTA." *See Hybrid Hearing before the Task Force on Financial Technology of the Committee on Financial Services*, 117th Cong. 82 (2022) (Ex. G). Earlier this year, the Senate Banking Committee held similar hearings and again consumer advocacy groups pressed Congress to close the so-called "wire transfer loophole." (Ex.

H; Ex. I, at 22.) No one suggested at either hearing that the EFTA already placed consumer wires within its protections, as NYAG urges here.

It thus remains well understood that, unless and until Congress acts, the EFTA's coverage does not encompass consumer wire transfers. Indeed, in 2023, the *Chicago Sun-Times* published a lengthy feature on what it termed the "wire transfer loophole," noting that "[v]ictims and consumer advocates want to close the wire transfer loophole" in the EFTA. (Ex. J, at 12.)[5]

B. NYAG's Complaint

NYAG brings eight claims, all arising under Executive Law § 63(12), which authorizes NYAG to seek an injunction and damages for "repeated fraudulent or illegal acts." (Compl. ¶¶ 263-325.) The Complaint attempts to use Executive Law § 63(12) as a vehicle to pursue "illegal" or "fraudulent" conduct under other federal or state laws. The eight claims can be grouped into four categories: (1) EFTA claims; (2) UCC claims; (3) data security claims; and (4) consumer deception claims.

- **EFTA Claims**. NYAG's central allegation is that Citibank wrongly applies the UCC to consumer wires instead of the EFTA. NYAG separately alleges that there is an EFTA violation when scammers consolidate funds among a customer's accounts (*e.g*., transfers from savings to checking), and yet a further EFTA violation because Citibank's written customer agreements allegedly do not conform to the EFTA's requirements. (*Id.* ¶¶ 273-80.)

- **UCC Claims**. NYAG alleges, in the alternative, that Citibank violated UCC Article 4A by not employing commercially reasonable security procedures. (*Id.* ¶¶ 69, 288-97.)

- **Data Security Claims**. NYAG alleges that Citibank has violated the federal "Red Flags Rule" and New York's "SHIELD Act" because Citibank allegedly does not have in place sufficient procedures to detect and prevent scammers from succeeding in the types of fraud that worked in the cases of NYAG's example Consumers "A" through "J." (*Id.* ¶¶ 298-316.)

[5] The Court may take notice of the "fact" of "press coverage" of matters on a motion to dismiss, without regard for the truth of the coverage. *Staehr v. Hartford Fin. Servs. Gp., Inc*., 547 F.3d 406, 425 (2d Cir. 2008).

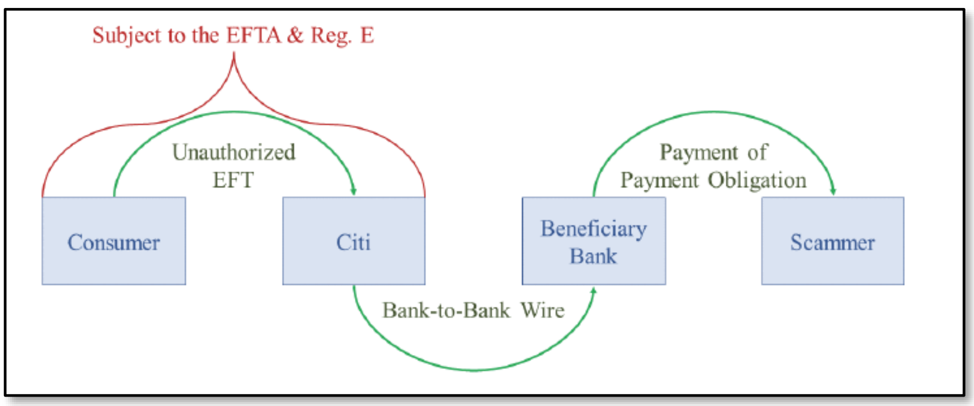
- **Consumer Deception Claims**. NYAG alleges fraudulent and deceptive conduct, in violation of Executive Law § 63(12) and New York's consumer protection law, N.Y. Gen. Bus. L. § 349, based on advertising statements such as "your security is important to us," and based on the manner in which Citibank handles fraud complaints. (*Id.* ¶¶ 84, 317-25.)

ARGUMENT

I. NYAG's First Cause of Action for "Unauthorized Debits" Under the EFTA Should Be Dismissed Because the Wire Transactions at Issue Are Exempt.

The core allegation of the Complaint is that Citibank commits "illegal acts," N.Y. Exec. L. § 63(12), when it applies UCC Article 4A in the circumstances of allegedly unauthorized online wire transfers, instead of the EFTA. (Compl. ¶ 62.)

According to NYAG's novel theory, a single wire transfer can be subdivided into at least three separate components, each potentially subject to different laws, as depicted by the below image from the Complaint (*see id.* ¶ 58):



As NYAG sees it, a wire transfer consists ***only*** of the "bank-to-bank" transmission of funds between institutions that subscribe to the wire services, even though those transmissions are necessarily predicated on the transaction's other interrelated components, *i.e.*, the sending bank debiting its customer, and the receiving bank crediting its customer.

Based on this artificial deconstruction of a wire transfer, NYAG argues that the sending bank's debit of its own customer is an independent, EFTA-covered transaction, which does not

trigger the consumer wire exemption. NYAG's theory is as imaginative as it is incorrect, and the Court should reject it for the multiple reasons discussed below.

A. The EFTA Exempts Consumer Wires.

As detailed above, the EFTA is absolutely clear that consumer wires are exempted. The statute defines "electronic fund transfer" to exclude transfers "***on behalf of a consumer*** by means of a [wire] service." 15 U.S.C. § 1693a(7)(B) (emphasis added). The Federal Reserve similarly explained when adopting Regulation E that the exemption was intended to carve out "transfers ***for consumers*** by any network similar to Fedwire." Electronic Funds Transfers, 44 Fed. Reg. 18,468, at 18,471 (Mar. 28, 1979) (emphasis added).

Ignoring these express references to "consumer" transfers, NYAG inaccurately describes the statutory exemption as a "narrow" exemption covering ***only*** the bank-to-bank component where funds go from "Citi's own accounts (not consumers' accounts)" to the "the beneficiary bank's own accounts." (Compl. ¶¶ 62, 97.) Under NYAG's characterization, the consumer is written out of the wire transfer. Yet, this interpretation violates "one of the most basic interpretive canons," namely, that a statute should be construed so that its terms are given effect, and that "no part will be inoperative or superfluous, void or insignificant." *Corley v. United States*, 556 U.S. 303, 314 (2009) (citation omitted). Under this fundamental interpretive principle, the term "consumer" cannot be erased, as NYAG is trying to do here.

Further, NYAG's reading of the EFTA would mean that the consumer wire exception ***never applies***, rendering it meaningless. As discussed, the EFTA applies only to transfers to or from accounts "established primarily for personal, family, or household purposes." 15 U.S.C. § 1693a(2), (7). If NYAG were correct that the consumer wire exemption is confined only to the transmission between the accounts of banks that interface with the particular wire service (*i.e.*, between two accounts that are not for "personal, family, or household" purposes), the exemption

expressly crafted by Congress would have been unnecessary because these transmissions would not be covered by the EFTA in the first instance.

The Court should reject NYAG's attempt to rewrite the EFTA.

B. The Regulatory Record Further Confirms that Consumer Wires Are Exempted From the EFTA.

Regulatory authority from multiple federal agencies (the Federal Reserve Board, the FDIC, and the CFPB) also makes it absolutely clear that the EFTA exempts consumer wires.

1. Federal Reserve Guidance Makes Clear That the Consumer Is Part of a Wire Transfer.

As discussed above, the Federal Reserve's official guidance in 1981 stated that transfers "sent by Fedwire or a similar network" with electronic "instructions for ***crediting individual consumers' accounts***" are subject to the wire transfer exemption. Electronic Fund Transfers, 46 Fed. Reg. 46,876, at 46,879 (Sept. 23, 1981) (Question 3-2) (emphasis added). This Guidance cannot be squared with NYAG's theory that the bank-to-bank component stands alone because, if that were so, there would be no relevance to the subsequent "crediting [of] individual consumers' accounts." The Guidance refers to the ultimate payee because the payment, from sender to recipient, is appropriately treated as one transfer.

That same Guidance helpfully provides an example of when a series of payments ***would*** be considered as separate for EFTA purposes: a "company sends funds by Fedwire or a similar network from one financial institution to another, and transfers via ACH are then made from the second institution to the accounts of company employees at ***still other institutions***." *Id.* at 46,879 (Question 3-3) (emphasis added). The Federal Reserve explained that "[a]lthough the Fedwire transfer is exempt, the ACH transfers to employees' accounts are subject to" the EFTA. *Id.*

This example illustrates that when there is a sequence of payments where one leg of the payment is via one mechanism (*e.g.*, wire) and the next via another (*e.g.*, ACH), the different

mechanisms can be regulated differently. But, tellingly, there is no indication that the internal crediting or debiting ***within*** any particular payment mechanism—that is, the internal means banks use to ***carry out*** the wire or ACH payment—is ever treated as a separate EFTA transfer.[6]

Finally, the Federal Reserve's commentary to Regulation J (the regulation governing Fedwire, discussed above) specifies that "Fedwire funds transfers ***to or from consumer accounts*** are exempt from the EFTA and Regulation E." 12 C.F.R. pt. 210, subpt. B, app. A (commentary to § 210.25(b)(4) (emphasis added)). It is notable that the Federal Reserve is again characterizing for EFTA purposes the transfers as payments to or from consumer accounts—that is, treating the full wire transfer as one—and not confusing matters, as NYAG is attempting to, by artificially separating out banks' internal settlement or execution mechanisms.

2. The FDIC's Guidance Is That the Wire Exemption Applies to Consumer Wires.

Another agency that agrees with the effect of the wire exemption is the FDIC. In 1994, the FDIC issued an interpretive letter addressing whether it was proper for a bank to charge a $35 fee when a consumer tried to wire "$200 from Germany to her grandson in Arizona," but the bank misdirected the wire. *See* FDIC, *Users' Rights Under the Electronic Funds Transfer Act in the Event of Bank Error Regarding an Electronic Wire Transfer*, 1994 WL 393720, at *1 (1994). The FDIC noted that the EFTA exempts transfers through wire systems "such as the one which the German bank employed to transfer funds to the bank in Arizona," and so, the FDIC concluded, the issue was governed by Article 4A. *Id*.

[6] The current Regulation E guidance reflects this same understanding, describing a transfer which is a combination of Fedwire ***and*** ACH: "If a financial institution makes a fund transfer to a consumer's account after receiving funds through Fedwire or a similar network, the transfer by ACH is covered by the regulation even though the Fedwire or network transfer is exempt." *See* 12 C.F.R. pt. 1005, supp. I, Comment 3(c)(3)-1. If an ordinary Fedwire transfer ***alone*** triggered the EFTA's protections, one would expect this part of the Guidance to have simply said so.

3. CFPB Guidance Following the Dodd-Frank EFTA Amendments Confirms That the Wire Exemption Means What It Says.

Further confirmation that the EFTA does not mean what NYAG claims can be found in the history associated with Congress's decision in 2010 to extend certain protections of the EFTA to "remittance transfers," *i.e.*, transfers by domestic individuals to others abroad, as part of the law commonly known as "Dodd Frank." *See* Pub. L. 111-203 § 1073 (2010) (codified at 15 U.S.C. § 1693*o*-1). In adopting its final rule amending Regulation E, the CFPB stated plainly that it was taking remittance transfers via wire out of Article 4A, which otherwise ***would*** cover consumer wires:

> Consumers **currently receive some protections under UCC Article 4A** in the event the wire transfer is not completed, or in the event of errors in execution of the transfer, or **in connection with an unauthorized transfer**. Nonetheless, although **consumers who request wire transfers that are remittance transfers may no longer have the protections set forth in UCC Article 4A**, these consumers will receive error resolution, refund and cancellation rights and other protections for these transfers as set forth in [the updated Regulation E].

See Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 6,194, at 6,212 (Feb. 7, 2012) (emphasis added). If NYAG's interpretation were correct, then these wire remittances would ***already*** have been covered by the EFTA, and the amendments would have been unnecessary.[7]

Consistent with this point, the CFPB further explained that, until the Dodd-Frank amendments, the two "categories of transfers . . . believed to compose the majority of the remittance transfer market" were ***not*** previously covered by the EFTA: (1) transfers via money transmitters and (2) wire transfers. *Id.* at 6,195. Money transmitter transactions were not covered by the EFTA because they involve in-person cash payments (not debits of accounts initiated

[7] Although the Dodd-Frank amendments applied certain EFTA protections (*e.g.*, added disclosures) to remittance transfers, the refund protections at issue here apply only if the remittance transfer is also an "electronic fund transfer," which, as discussed, excludes wires. 12 C.F.R. § 1005.33(f)(3).

electronically), and remittances that consumers sent by wire were not covered because, as the CFPB observed, and as relevant here, "Congress had ***specifically structured the EFTA to exclude wire transfers***." *Id*. (emphasis added). The CFPB thus again recognized that the wire exemption has long operated to prevent consumer wires from falling within the EFTA.

The CFPB was not alone in that view. In 2012, the New York legislature amended the UCC to address certain spillover effects of Dodd-Frank, and, in describing the statutory backdrop, the State Assembly Memorandum accompanying the bill recognized that wires through Fedwire and CHIPS are "governed by Article 4A ***even if they involved consumers***." N.Y. Bill Jacket, L. 2012, Ch. 399, at 9-10 (emphasis added).

The UCC's Official Comments to the amendments echoed this same view:

> A ***consumer originates a payment order*** from the consumer's account at Bank A to the designated recipient's account at Bank B located outside the United States. Bank A uses the CHIPS system to execute that payment order. The funds transfer is a 'remittance transfer' as defined in 15 U.S.C. Sec. 1693*o*-1. ***This transfer is not an 'electronic fund transfer'*** as defined in 15 U.S.C. Sec. 1693a(7) ***because of the exclusion for transfers through systems such as CHIPS*** in 15 U.S.C. Sec. 1693a(7)(B) . . . .

Uniform Law Annotated, U.C.C. § 4A-108, Comment 2, Case #3 (emphasis added).

* * *

NYAG's theory amounts to claiming that it knows federal banking law better than federal banking regulators, such as the Federal Reserve, the FDIC and the CFPB. The Court should reject NYAG's implausible and incorrect claim.

C. The Monthly Statement Requirements in the EFTA and Regulation E Are Rendered Senseless Under NYAG's Theory.

"Statutes should be interpreted 'as a symmetrical and coherent regulatory scheme.'" *Mellouli v. Lynch*, 575 U.S. 798, 809 (2015) (citation omitted). Yet the EFTA's monthly disclosure requirements would make no sense if wires are subdivided, as NYAG proposes.

Under the EFTA, monthly consumer statements must disclose "the identity of any third party to whom or from whom funds are transferred." 15 U.S.C. § 1693d(a)(3), (c)(1). The House Report for the EFTA pointed out that this requirement was important so that customers could "easily recognize" their payments and "look for errors." H.R. Rep. No. 95-1315, at 8 (1978). Regulation E reflects this same requirement, and the Official Guidance is clear that, where "a consumer makes an electronic fund transfer to another consumer, the financial institution must identify the recipient by name." 12 C.F.R. § 1005.9 & pt. 1005 supp. I, Comment 9(b)(1)(v)-2.

Recognizing reality, these requirements treat a transaction where one consumer pays another as a ***single*** fund transfer to be disclosed, complete with the name of the ultimate recipient. If NYAG's view were adopted, however, and the internal debit/credit components of a wire were treated as standalone EFTA-covered transfers, then banks would be required by law to issue monthly statements listing ***the bank itself*** as the "recipient" every time a consumer initiates a wire transfer—defeating the purpose of the disclosure requirement.

D. There Is No Hint of NYAG's Novel Theory in the Nearly Half Century Since the EFTA's Passage.

The existence of a longstanding consensus as to the EFTA's meaning is powerful confirmation that the consensus understanding—and not a novel, hidden one—is correct. The Supreme Court's decision in *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142 (2012), illustrates this commonsense principle. *Christopher* considered whether the Fair Labor Standards Act's overtime rules applied to certain pharmaceutical sales representatives, who across the industry were considered exempt because they did "not punch a clock" like hourly workers and "often work[ed] more than 40 hours per week." *Id*. at 158. The Supreme Court acknowledged that although it was theoretically "possible for an entire industry to be in violation of the FLSA

for a long time without" anyone noticing, the far more "plausible hypothesis" was that the industry was acting lawfully all along. *Id.* (brackets and quotation marks removed).

Here, the EFTA has been on the books since 1978, but there has been no case law, regulatory or administrative guidance, nor any other authority, adopting NYAG's newly-crafted theory in the intervening 46 years. As discussed, regulators have consistently recognized that the EFTA's consumer wire transfer exemption, unsurprisingly, exempts consumer wire transfers. Courts have recognized the same point, as well.

The decision in *Fischer & Mandell LLP v. Citibank, N.A.*, 90 Civ. 1160, 2009 WL 1767621 (S.D.N.Y. June 22, 2009), is illustrative. Judge Sullivan dismissed EFTA claims against Citibank because "Regulation E explicitly excludes from the coverage of the EFTA transfers of funds made through checks and wire transfers," and there was "no dispute that each of the transactions at issue was made through checks and wire transfers." *Id*. at *3-4. And, in *Wright v. Citizen's Bank of E. Tennessee*, 640 F. App'x 401 (6th Cir. 2016), when a couple accused its bank of making an error in a wire payment, the Sixth Circuit dismissed the EFTA claim, holding: "Here, the funds transfers at issue were made through Fedwire. Therefore, the EFTA does not apply." *Id*. at 404. The court proceeded to analyze the claim under Article 4A. *Id*. at 404-07.[8]

Tellingly, as discussed, even consumer advocates have not advanced NYAG's theory, which is why they are lobbying Congress to adopt a proposed amendment to provide the

[8] *See also*, *e.g.*, *Pope v. Wells Fargo Bank, N.A.*, No. 2:23-cv-86, 2023 WL 9604555, at *3-4 (D. Utah Dec. 27, 2023) (EFTA claims by consumer who fell for "phishing" scam dismissed because the "EFTA is not applicable to wire transfers"); *Trivedi v. Wells Fargo Bank, N.A.*, 609 F. Supp. 3d 628, 633 (N.D. Ill. 2022) (declining to apply Regulation E to allegedly fraudulent consumer wire because UCC Article 4A governs "when the transaction involves a wire transfer"); *McClellon v. Bank of Am., N.A.*, No. C18-0829-JCC, 2018 WL 4852628, at *5 (W.D. Wash. Oct. 5, 2018) (holding that plaintiff stated a claim under UCC Article 4A but not the EFTA, since "Regulation E does not apply to '[w]ire or other similar transfers'" (quoting 12 C.F.R. § 1005.3(c)(3))); *Stepakoff v. Iberiabank Corp*., 637 F. Supp. 3d 1309, 1313 (S.D. Fla. 2022) (concluding that the EFTA did not apply to a requested wire transfer); *Bodley v. Clark*, No. 11 CIV. 8955 KBF, 2012 WL 3042175, at *4 (S.D.N.Y. July 23, 2012) (noting that "wire transfers are explicitly excluded from EFTA's definition of 'electronic fund transfers'").

outcome NYAG—improperly—seeks to accomplish via litigation. These legislative efforts undermine NYAG's claim that the EFTA's wire exemption ***already*** accomplishes what the proposed amendment would do. (Compl. ¶ 62 (alleging that consumer wire exemption is "inapplicable" to consumer wires and governs only bank-to-bank transmissions).) *See*, *e.g.*, *In re Thomas*, 931 F.3d 449, 455 (5th Cir. 2019) (citing proposed legislative amendments that sought "to make student loans dischargeable" as evidence that existing law should not be read as already making student loans easily dischargeable); *MED Trends, Inc. v. United States*, 102 Fed. Cl. 1, 6 (Fed. Cl. 2011) (inferring from "proposed legislation" that "Congress understands that the existing . . . provision does not accomplish the same result").

Beyond Congress and consumer groups, NYAG's theory has also eluded academic industry experts, who consistently describe the EFTA's consumer wire exemption as applying to consumer wires, without any hint of NYAG's novel theory:

- "[A]n electronically initiated wire transfer either from or to a consumer is excluded by Section 1005.3(c)(3) because it is sent via Fedwire or a similar network." 1 Benjamin Geva, *The Law of Electronic Funds Transfers* § 6.04 (2023).

- "Fedwire and CHIPS transactions are excluded from the EFTA even though the transfer is effected for a consumer. As to these transactions, Article 4A is applicable even though the transaction involves a consumer." 7 *Anderson on the Uniform Commercial Code* § 4A-108:5 (3d. ed. 2023).

- "If the EFT at issue is similar to the one discussed . . . (*e.g.*, an instruction from one entity to its bank to make a wire transfer payment to another entity's bank account that is conducted through the Federal Reserve), the transaction initially falls squarely under Article 4A. This is the case regardless of whether the originator is a consumer or a commercial entity due to the express language excluding these types of transactions from the EFTA and Regulation E." 3 White, Summers, & Hillman, *Uniform Commercial Code* § 22:2 (6th ed. 2023).

See also n.4, *supra* (collecting legal authorities from shortly after the adoption of Article 4A).

This shared and consistent understanding—spanning decades and among a wide range of courts, industry experts, consumer groups, regulators and others—underscores that the EFTA should not be given the unique interpretation that NYAG advances.

E. In the Alternative, the EFTA's "Automatic Transfer" Exemption Defeats NYAG's Claim.

Even if the Court were to adopt NYAG's unprecedented division of wire transfers into separate "electronic funds transfers," its theory would still fail under the EFTA's "automatic transfer" exemption. Regulation E explicitly exempts from the EFTA's coverage certain automatic intra-bank transfers, including:

> Any transfer of funds under an agreement between a consumer and a financial institution which provides that the institution will initiate individual transfers without a specific request from the consumer . . . [b]etween a consumer's account and an account of the financial institution.

12 C.F.R. § 1005.3(c)(5). Thus, under this exemption, if a consumer agrees that an internal debit will occur "automatically on the occurrence of certain events"—say, a payment every month when a mortgage payment is due—the EFTA does not apply. *See* 12 C.F.R. pt. 1005, supp. I, Comment 3(c)(5). Here, the Complaint alleges (correctly) that, by operation of Citibank's customer account agreements, a debit from the customer's account is ***automatically*** approved when a wire is requested. (Compl. ¶ 56.) Consistent with the notion of a consumer wire as a single, integrated transaction, Citibank's Client Manual and Deposit Account Agreement—both of which are incorporated into the Complaint (*see* Compl. ¶¶ 42, 77-78)[9]—provide that "[w]hen you request a funds transfer, you authorize [Citibank] to debit your account for the amount of the transfer . . . ." (*See* Ex. K, at 21; *see also* Ex. L, at 60 (similar language).)

---

[9] The Court may consider on a motion to dismiss "documents incorporated in the complaint by reference." *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 191 (2d Cir. 2007).

There is no allegation, nor could there be, of a customer having to provide ***two*** approvals, one for the debit, and one for the bank-to-bank transmittal. There is instead a standing instruction to initiate the internal debit from the customer's account upon the occurrence of a wire request. This procedure fits the plain language of the exemption exactly, no differently than, for example, a standing instruction to deduct the minimum payments on a credit card and letter of credit each billing cycle. *See Krutchkoff v. Fleet Bank, N.A.*, 960 F. Supp. 541, 543-44 (D. Conn. 1996) (applying exemption to that fact pattern). On this independent basis, NYAG's EFTA claim fails.

II. NYAG's Second Cause of Action Should Be Dismissed Because "Intra-Bank Transfers" Are Not "Unauthorized" and Cause No Losses for NYAG to Recover.

In a further attempt to stretch the EFTA beyond its text and purpose, NYAG alleges that unauthorized electronic fund transfers between a single customer's accounts (*e.g*., from savings to checking) that precede a fraudulent wire are EFTA-covered transfers requiring reimbursement. (Compl. ¶¶ 277-79.) Under the EFTA, however, a transfer "from a consumer's account" is only considered "unauthorized," and thus eligible for reimbursement, if a person without authority initiates it and the "consumer receives no benefit." 15 U.S.C. § 1693a(12).

In the case of a transfer across one consumer's accounts, the consumer receives the transferred funds and therefore ***does*** receive the benefits. Thus, in *Becker v. Genesis Fin. Servs*., CV-06-5037, 2007 WL 4190473, at *12 (E.D. Wash. Nov. 21, 2007), a consumer claimed she "did not give permission" to a credit card company to transfer a balance to another one of her cards, but the court ruled the transfer was not "unauthorized" because she received the benefit of the transfer. *Id*. at *12. Similarly, when a credit card company deducted funds from a consumer's bank account, allegedly without permission, the Second Circuit held the transfer was not "unauthorized" because the consumer received the "benefit of reducing her debt." *Aikens v. Portfolio Recovery Assocs., LLC*, 716 F. App'x 37, 40 (2d Cir. 2017). So too here, where the

outflow of money from one account corresponds to an equal credit—a benefit—to the consumer in another. This result is consistent with the language and structure of the EFTA, which refers to banks having to "reimburse[]" the "consumer for losses" arising from unauthorized transfers. 15 U.S.C. § 1693g(2). This language presumes that the consumer has lost money that can be reimbursed—which does not make sense in contexts like this one, where there is no "loss."

Relatedly, NYAG fails to plead facts justifying its claimed remedy—"restitution and damages" for persistently fraudulent or illegal conduct, N.Y. Exec. L. § 63(12)—because, in these circumstances, there is nothing to recover or enjoin. Any loss is not caused by the transfer between the customer's accounts but rather by the subsequent outbound wire transfer. New York courts have consistently held that where funds are first transferred among a customer's own accounts and then converted from the receiving account, the relevant injury arises from the conversion rather than the transfer between accounts. *See Davis Aircraft Prod. Co. v. Bankers Tr. Co.*, 319 N.Y.S.2d 379, 379-80 (1st Dep't 1971); *Rizer v. Breen*, No. 601676/05, 2007 WL 4378149, at *15 (N.Y. Sup. Ct. Jan. 29, 2007).

III. NYAG Fails to Plead Any Disclosure Violations or "Illegal Agreements," Defeating the Third Cause of Action.

The Third Cause of Action advances two separate claims as to alleged deficiencies in Citibank's customer disclosures and agreements. The Court should reject both.

A. There Is No Obligation for Citibank to Detail Its "Security Protocols."

The EFTA requires banks "at the time the consumer contracts" for a covered service to make certain disclosures in "readily understandable language," such as who to contact about fraud and what fees will be charged. 15 U.S.C. § 1693c; 12 C.F.R. §§ 1005.4, 1005.7. ***Nowhere*** does the EFTA, as NYAG alleges, require Citibank "to describe in clear and readily understandable terms the security protocols that Citibank will actually deploy to prevent

unauthorized EFTs initiated via online or mobile banking." (Compl. ¶¶ 283, 285.) Indeed, the requirements mention ***nothing*** about disclosing security protocols—and for good reason. 15 U.S.C. § 1693c; 12 C.F.R. § 1005.7. Doing so would provide a roadmap for fraudsters.[10]

B. Citibank's Account Agreements Do Not Waive Rights Under the EFTA.

The Court should reject the Third Cause of Action's claim that Citibank's online customer agreement (the "Online Agreement") violates the EFTA's "anti-waiver" provision (*see* Compl. ¶ 286), which states:

> No writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created by [the EFTA].

15 U.S.C. § 1693*l*. NYAG's three theories on this point are all meritless.

First, NYAG alleges that Citibank treats a transaction "initiated through online or mobile banking using usernames and passwords as an authorized EFT even if not made with actual authority." (Compl. ¶ 286(a).) This apparently refers to a clause in Citibank's Online Agreement stating that Citibank is authorized to treat instructions authenticated via a username and password "as if the instructions had been made in writing and signed by you." (Ex. M, at 3 (§ G).) But NYAG does not allege that Citibank actually reads or applies this clause to waive any EFTA rights, or that it has ever been applied to deny reimbursement based on an unauthorized person only having access to the customer's username and password. Belying NYAG's allegations, the scams cited by NYAG are far more sophisticated, involving, for example:

- a customer whose personal information, including social security number, was stolen from a mortgage firm (Consumer B) (*see* Compl. ¶ 154);

[10] Relatedly, daily ATM withdrawal limits generally must be disclosed unless their "confidentiality is necessary to maintain the security of an electronic fund transfer system." 15 U.S.C. § 1693c(a)(3). Clearly, if the EFTA's drafters believed that merely disclosing matters such as ATM withdrawal limits could present an unacceptable security risk, then there cannot be a separate, undisclosed, affirmative requirement implied in the statute to spell out the precise security procedures employed by a bank for verification of wire transfer requests.

- a customer who provided a scammer the answers to three security questions (Consumer F) (*see id*. ¶ 184); and
- a customer who read the scammer her debit card number and codes texted to her over the phone (Consumer J) (*see id*. ¶ 237).

Put simply, the notion that Citibank forces customers to agree to waive their EFTA protections in the manner NYAG alleges is refuted by the Complaint itself.

Second, NYAG alleges that the Online Agreement's terms have "altered Citi's burden of proof by contractually providing that Citi may treat its own internal records and documents as conclusive evidence." (Compl. ¶ 286(b).) Contrary to NYAG's characterization, the Online Agreement plainly does not shift any burdens. The relevant provision states only that Citibank's own business records will ordinarily be conclusive proof as to what those records show occurred: "Unless there is substantial evidence to the contrary, Citibank records will be ***conclusive regarding any access to, or action taken through, Citi Online***." (Ex. M, at 3 (§ G) (emphasis added).) This provision is, effectively, an evidentiary presumption about Citibank's business records. If, for example, Citibank's records showed that a wire was authorized in part by email, then those records would ordinarily be "conclusive" that an email was sent as the records show, nothing more. This presumption does not relieve Citibank of any statutory EFTA obligations.

Third, NYAG advances an equally untenable variation of this argument by alleging that the Online Agreement alters "Citi's obligations to undertake a reasonable investigation under the EFTA and Reg. E, instead providing that Citi may deem its records 'conclusive' in the absence of 'substantial' contrary evidence." (Compl. ¶¶ 89, 286(c).) Again, this argument is defeated by the Online Agreement's plain language. The modest presumption that Citibank's own records are reliable does not somehow mean that Citibank is attempting to short circuit any obligation to undertake reasonable investigations.

IV. NYAG Does Not Plead Facts Showing UCC Violations, Defeating the Fourth Cause of Action.

NYAG's UCC-based claim (Compl. ¶¶ 288-97) is not brought directly under the UCC but, again, arises under the Executive Law's prohibition against "repeated . . . illegal acts." N.Y. Exec. L. § 63(12). In other words, NYAG uses the Executive Law here as "only a mechanism" to "show that injunctive relief and restitution are proper" for alleged Article 4A violations. *People ex rel. Schneiderman v. One Source Networking, Inc*., 3 N.Y.S.3d 505, 508 (4th Dep't 2015).

This is a particularly important distinction for the UCC-based claim because it is not "illegal" under the UCC for Citibank to have antifraud practices that NYAG believes are inadequate, which seemingly is the overarching theme of NYAG's UCC claim. Rather, the reasonableness of Citibank's security procedures must be considered in connection with specific unauthorized wire transfers. For NYAG to meet its burden of pleading "repeated" and "illegal" conduct, the facts as alleged must actually add up to multiple, particular instances of Citibank violating the UCC by, for instance, refusing to pay refunds that are due, or by sending wires in contravention of consumer instructions. Yet, NYAG wholly fails to meet its burden to plead facts essential to that showing. The Fourth Cause of Action thus should be dismissed.

A. The Governing UCC Standards Require Only that Security Procedures Be Commercially Reasonable and that a Bank Act in Good Faith and in Compliance with the Procedures.

UCC Article 4A provides that banks are not responsible to reimburse unauthorized online funds transfers if (1) the bank and the customer have agreed to a "commercially reasonably security procedure" and (2) the bank "accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." N.Y. U.C.C. §§ 4-A-202(2), 4-204(1). A "security procedure" is a "procedure established by agreement of a

customer and a receiving bank for the purpose of . . . verifying that a payment order or communication amending or cancelling a payment order is that of the customer." N.Y. U.C.C. § 4-A-201.

The commercial reasonableness of security procedures is "a question of law," so as to ensure "more predictability." N.Y. U.C.C. § 4-A-203, Official Comment 4. These standards are intended to "encourage banks to institute reasonable safeguards against fraud," but that does not "make them insurers against fraud." *Id*. Further, a "security procedure is not commercially unreasonable simply because another procedure might have been better[.]" *Centre-Point Merchant Bank Ltd. v. Am. Express Bank Ltd*., No. 95 Civ. 5000, 2000 WL 1772874, at *4 (S.D.N.Y. Nov. 30, 2000) (citation omitted).

The decision in *Braga Filho v. Interaudi Bank*, No. 03 Civ. 4795, 2008 WL 1752693 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 334 F. App'x 381 (2d Cir. 2009), is illustrative. In *Filho*, a couple sued their bank when 17 unauthorized wires totaling $950,000 were made from their account via fax requests. The court, applying Article 4A, ruled for the bank because there was an agreement for a security procedure, which the bank followed in good faith. *Id*. at *4-5. The agreement was a flexible one, allowing the bank to "select security procedures for accepting instructions that [were] commercially reasonable for" the bank. *Id*. at *4. The security procedure the bank chose and actually deployed in these instances was one that the court agreed was commercially reasonable—namely, the bank (1) compared the signature on the faxes with a signature card on file, (2) called the customer's number to confirm the answers to security questions (*e.g*., mother's maiden name), and (3) recorded and logged the call. *Id*. at *4. As the court observed, "[w]hoever made these requests had access to all the necessary information" to pass the security procedures, which meant the bank was not responsible. *Id*. at *5.

B. NYAG Fails to Allege Facts Describing the Security Procedures or Why They Were Allegedly Deficient.

The Online Agreement allows Citibank, like the bank in *Filho*, flexibility in selecting the appropriate security procedure, which can involve email, telephone, or other customer contact:

> Citi Online has been designed to reduce the possibility of fraud and error by placing the issuance of a User ID, and Passwords ("Codes") under your control so that your accounts may be accessed only upon entry of valid Codes. You authorize Citibank to treat any instruction made on Citi Online with valid Codes as if the instructions had been made in writing and signed by you.
>
> . . .
>
> When you place an order for a funds transfer (including a wire or cable transfer), Citibank ***may follow a security procedure established for your protection that may entail a telephone call or other required contact*** with or from you prior to acting upon your instructions. In certain instances, Citibank may also decline to act upon your instructions. ***Citibank may employ other controls to verify your identity*** . . . .
>
> ***You agree to these security procedures***, and acknowledge that if contacted, either by telephone or electronically, you will act or respond in compliance with requests resulting from these security procedures . . . .

(Ex. M at 3 (§ G) (paragraph break and emphasis added).) The reason that the Online Agreement affords Citibank flexibility is self-evident: widely available, standardized consumer banking agreements that spell out exactly how a bank verifies wires—or, worse, that specify that a singular procedure will ***always*** be deployed—would provide a roadmap for fraudsters and would limit a bank's ability to use ever-changing methods that are harder for fraudsters to anticipate.

This is the industry approach in consumer banking. Indeed, the court in *Filho* explained that it was perfectly appropriate that customers "did not know what the Bank's security procedures were," because the bank would have every incentive to deploy one that is commercially reasonable. *Filho*, 2008 WL 1752693, at *4; *see also Chavez v. Mercantil Commercebank, N.A.*, 701 F.3d 896, 902 (11th Cir. 2012) (noting that a bank could "select the security procedure" so long as the customer "granted to the bank the right to" do so). Citibank's

competitors similarly do not spell out in their standardized agreements exactly how wires or other transfers will be confirmed.[11]

Failing to appreciate this point, NYAG alleges Citibank has commercially unreasonable procedures because the Online Agreement "incorporate[s] single-factor authentication," under which a name and password will suffice. (Compl. ¶ 293(a).) But the Agreement's terms themselves show otherwise. Although the Online Agreement states that Citibank may treat instructions via a username-and-password method "as if the instructions had been made in writing and signed by you," it is clear that this is ***not*** the only procedure deployed. The Online Agreement goes on to describe additional security procedures that "may entail a telephone call or other required contact," among "other controls" for the customer's protection. (Ex. M at 3 (§ G).)

NYAG's UCC allegations fail to set forth which of these additional identity-verification procedures were employed that led to payments being approved in specific cases—in other words, the facts bearing on the reasonableness of the procedures that Citibank used. Although ***some*** aspects of the procedures can be inferred from the descriptions of the transactions, those clues are a far cry from factual allegations about what procedures were employed or why they were lacking. In fact, Citibank employs robust security procedures. *See*, *e.g.*, *In re Bhuya v. Citibank, N.A.*, No. 23CV07082, 2023 WL 7286783 (E.D.N.Y. Sept. 22, 2023) (arbitral award in Citibank's favor where scammers passed security procedures because they "had access to the

[11] *See* Ex. N, at 12 (Bank of America customer agreement stating that customers agree to "security and identification methods as we may require from time to time"); Ex. O, at 81 (Chase customer agreement stating: "When you use this service, you will authenticate with a username and password and may, from time to time, be asked to complete additional authentication steps like security questions, one-time codes, and other methods of authentication."); Ex. P, at 31 (Wells Fargo customer agreement stating: "The Security Procedure consists of verifying your username and a password, and/or such other additional security and authentication methods as we may require from time to time."). These terms are judicially noticeable. *See McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 600 n.2 (S.D.N.Y. 2020) (taking judicial notice of non-party's "publicly accessible" online terms of use where there was no dispute as to authenticity or existence of the terms of use).

log-in information," had access to "the full debit card number and pin," and responded to fraud alerts with "the last four digits of the Claimant's social security number").

NYAG next alleges that Citibank lacks "mechanisms to identify high-risk transactions or anomalous behavior," such as wires that would empty accounts. (Compl. ¶¶ 293(a), (b).) In fact, Citibank ***does*** have robust mechanisms to identify suspicious transactions, but, even taking the allegation as true, NYAG misconstrues the law. The term "security procedure" does not refer to a bank's overall risk matrix for approving wires or to other "procedures that the receiving bank may follow unilaterally in processing payment orders." N.Y. U.C.C. § 4-A-201, Official Comment 1. The term is instead defined as the procedure for "verifying that a payment order or communication amending or cancelling a payment order is that of the customer." N.Y. U.C.C. § 4-A-201. That is, a security procedure is simply how a bank verifies that the sender of a wire is who he or she claims to be—which is what NYAG fails to allege.

The Eighth Circuit's decision in *Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir. 2014), is instructive regarding this distinction. In that case, a business fell victim to a phishing scam that ultimately led to $440,000 being wired to an unknown account in Cyprus. *Id*. at 613. Upholding a finding that the bank's security procedures were commercially reasonable, the Eighth Circuit held that the bank was ***not*** required to incorporate into its procedures a "transactional analysis" that would flag "irregularities" based on the "size, type, and frequency" of each payment. *Id*. at 619. This "foreign standard" did not match the UCC's description of security procedures as customer-verification tools like "algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices." *Id*.; *see* N.Y. U.C.C. § 4-A-201 (listing these examples).

Drawing this line makes practical sense. It cannot be, as NYAG suggests, that every individual dispute over an unauthorized payment opens the door to examining and second-guessing the complex algorithms and systems banks use to flag suspicious transactions—as opposed to the more cabined and relevant inquiry of how the bank chose in each instance to verify that the particular payment order came from its customer. The UCC's guidance that commercial reasonableness is to be decided as "a matter of law" to provide "predictability," N.Y. U.C.C. § 4-A-203, Comment 4, is wholly undermined if every dispute over an unauthorized transaction can morph into a referendum on how a bank detects and blocks fraud generally.

NYAG makes a similar error in alleging that Citibank lacks sufficient controls and training to "respond effectively in real-time to reject fraudulent Payment Orders." (Compl. ¶ 293(c).) The question of how rapidly Citibank ***responds*** to detected fraud is plainly different from the issue of how it may verify a customer's identity.

To be sure, Citibank has every incentive to employ, and ***does*** employ, robust procedures for identifying suspicious transactions, and Citibank trains its staff to detect and stop fraud. Where the Complaint goes awry is when it tries to turn the UCC's security procedure concept into a toehold for regulating through litigation the overall antifraud practices of the banking industry. The upshot of this fundamental legal error is that NYAG fails to meet its burden of including factual allegations pertinent to the governing legal standard for a security procedure. Its claim should therefore be dismissed. *Trivedi v. Wells Fargo Bank, N.A.*, 609 F. Supp. 3d 628, 632 (N.D. Ill. 2022) (dismissing Article 4A claim where plaintiff had "not alleged that either Defendant has failed to implement a security procedure").[12]

[12] For the same reasons, NYAG's passing allegation that Citibank did not act in "good faith" (Compl. ¶ 294)—referring to the requirement for the bank to have "accepted the payment order in good faith," N.Y. U.C.C. § 4-A-202(2)—should be rejected. Absent allegations as to the ***grounds*** for accepting a particular payment order, it is impossible to state a claim premised on that decision being one made in bad faith.

C. NYAG Also Does Not Allege That Citibank Failed to Honor Customer Instructions Restricting Acceptance of Payment Orders.

The final aspect of NYAG's Fourth Cause of Action focuses on the UCC provision that banks bear the responsibility for unauthorized wires if they do not comply with "any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." N.Y. U.C.C. § 4-A-202(2). The UCC explains: "the customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount." N.Y. U.C.C. § 4-A-203, Official Comment 3.

The Complaint contains no allegation of a customer issuing any particular "instruction" that "restrict[ed]" the "acceptance of payment orders," much less an allegation that Citibank countermanded any particular instruction. N.Y. U.C.C. § 4-A-202(2). NYAG alleges instead that Citibank violates this clause by improperly accepting payment orders in the face of "red flags" of fraudulent activity, and by "delay[ing]" efforts to recover stolen funds. (Compl. ¶ 294.) However, once again, NYAG strays far from the actual legal standards, seeking to impose obligations that simply are not in the law. The practices about which NYAG complains plainly are not the same as defying a consumer instruction; this claim should be dismissed.

V. The Sixth Cause of Action, Based on the Red Flags Rule, Is Both Preempted and Inadequately Pleaded.

NYAG's claim based on the Red Flags Rule, a federal identity theft regulation, must be dismissed because (1) the FCRA prevents enforcement by state agencies or through state laws, such as the vehicle for NYAG's claim, Executive Law § 63(12); and (2) the Complaint lacks sufficient facts to show that Citibank failed, as the Rule requires, to develop and implement an identity theft policy. The Court should therefore dismiss the Sixth Cause of Action.

A. The Red Flags Rule Requires Banks and Others to Adopt Policies to Combat Identity Theft.

The origins of the Red Flags Rule go back to 2003, when Congress, amending the FCRA, directed a group of agencies to jointly "establish and maintain guidelines. . . regarding identity theft," and to "prescribe regulations" requiring banks "to establish reasonable policies and procedures for implementing the guidelines." Pub. L. 108-159 § 114 (2003) (codified at 15 U.S.C. § 1681m(e)). "Identity theft" is defined as "fraud committed using the identifying information of another person." *Id*. § 111.

Nothing in the statute imposes liability whenever a fraudster's identity theft scheme succeeds. The resulting regulation—the Red Flags Rule—requires a covered bank to "***develop and implement*** a written Identity Theft Prevention Program (Program) that is ***designed*** to detect, prevent, and mitigate identity theft . . . ." 12 C.F.R. § 41.90(d) (emphasis added). A bank's Program must "include reasonable policies and procedures" to "[i]dentify relevant Red Flags" in "covered accounts," and "Red Flag" is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." 12 C.F.R. § 41.90(b)(10), (d)(2)(i).

B. The FCRA Preempts NYAG's Claim Under New York Executive Law Section 63(12).

NYAG's claim under the Red Flags Rule must be dismissed because the FCRA expressly precludes NYAG from enforcing the Red Flags Rule directly, *see* 15 U.S.C. § 1681m(h)(8)(B) (enforcement "exclusively" via certain federal agencies and officials), and because the FCRA preempts NYAG's indirect claim under Executive Law § 63(12).

The relevant FCRA preemptive provision states that "[n]o requirement or prohibition may be imposed under the laws of any State . . . with respect to the conduct required by the specific provisions" of various FCRA provisions, including the one regarding the Red Flags Rule. 15 U.S.C. § 1681t(b)(5)(F) (covering, among other provisions, 15 U.S.C. § 1681m(e)).

Because preemption in this case is based on an express statutory provision (as contrasted with implied preemption), the "focus" is "on the plain wording of the statute, which is necessarily the best evidence of the scope of Congress's preemptive intent." *Galper v. JP Morgan Chase Bank, N.A.*, 802 F.3d 437, 443 (2d Cir. 2015).

The key phrase "[n]o requirement or prohibition" in § 1681t "sweeps broadly" to encompass both statutory and common-law claims. *Premium Mortg. Corp. v. Equifax, Inc.*, 583 F.3d 103, 106 (2d Cir. 2009) (citation omitted). Similarly, the phrase "***with respect to the conduct*** required," 15 U.S.C. § 1681t(b)(5)(F) (emphasis added), reflects Congress's intent to broadly preempt state law addressing conduct overlapping with matters covered by the enumerated federal provisions.

The decision in *Willey v. J.P. Morgan Chase, N.A.*, No. 09 Civ. 1397, 2009 WL 1938987 (S.D.N.Y. July 7, 2009), is compelling here. In *Willey*, a bank customer accused Chase of violating state law by failing to maintain reasonable procedures regarding the disposal of personal financial information, as required under 15 U.S.C. § 1681w. *Id*. at *1. Chase argued that the customer's state-law claims were preempted under 15 U.S.C. § 1681t(b)(5) because the claims related to the "conduct" required by the FCRA—specifically, the disposal of customer information under 15 U.S.C. § 1681w. Judge McMahon agreed, finding that Congress intended preemption in this context "to set uniform national standards" for how banks manage their data, which "implie[d] broad preemption of state law claims." *Id*. at *8. Since the state law claims focused on "conduct" already regulated by the federal law—namely, how banks dispose of customer data—those claims were preempted. *Id*.

Also persuasive is the reasoning in *Elias v. Synchrony Bank*, No. BC555883, 2016 WL 6270746 (Cal. Super. Ct. Oct. 25, 2016). In *Elias*, a consumer accused his bank of selling credit

card debt that he allegedly owed, while overlooking "red flags," including those in the Red Flags Rule, that should have shown that debt was part of an identity theft scam. *Id.* at *10-11. The consumer framed the claim as a state law invasion of privacy tort, claiming his personal information was disseminated in the sale. *Id.* at *10. The court found the claim preempted under 15 U.S.C. § 1681t(b)(5)(F) because the "statutory scheme specifically prohibits a state from adopting any requirement or prohibition governing" the Red Flags Rule, and the plaintiff was "essentially . . . attempting to enforce" the Red Flags Rule via state law. *Id.* at *11.

The same holds true here. Like the claims in *Willey* and *Elias*, NYAG's attempt to enforce the Red Flags Rule against Citibank through a state law, Executive Law § 63(12), fails as a matter of law. The claim is preempted.[13]

C. NYAG Additionally Fails to Plead Facts Showing Violations of the Red Flags Rule.

Even if not preempted (which it is), NYAG's claim under the Red Flags Rule should be dismissed because NYAG wrongly tries to transform the Rule's limited obligation to "develop and implement" a written policy "designed" to combat identity theft into a boundless obligation to catch every scammer every time. The Complaint accuses Citibank of violating the Red Flags Rule because it allegedly "has ***failed to ensure*** that Defendant's identity theft prevention

[13] NYAG cannot avoid preemption by asserting the Complaint is based on underlying violations of federal law. Indeed, numerous courts have held that the FCRA preempts state-law claims similar to those asserted by NYAG here. *See Manes v. JPMorgan Chase Bank, N.A.*, 20 Civ. 11059, 2022 WL 671631, at *5 (S.D.N.Y. Mar. 7, 2022) (finding negligence and GBL § 349 claims preempted under § 1681t(b)(1)(F), reasoning that "Plaintiff's negligence and § 349 claims are both preempted by FCRA because Plaintiff has not pled any facts to suggest that these claims concern conduct different from that underlying his FCRA claim"); *Munroe v. Nationstar Mortg. LLC*, 207 F. Supp. 3d 232, 240 (E.D.N.Y. 2016) (finding GBL § 349 claim preempted under 15 U.S.C. § 1681t(b)(1)(F)); *Reyes v. Downey Sav. & Loan Ass'n, F.A.*, 541 F. Supp. 2d 1108, 1115 (C.D. Cal. 2008) (holding that claim under California's Unfair Competition Law predicated on violations of federal Truth in Lending Act were preempted); *Howard v. Blue Ridge Bank*, 371 F. Supp. 2d 1139, 1143 (N.D. Cal. 2005) (holding that claim under "unlawful" prong of California's Unfair Competition Law based on underlying violation of the FCRA was preempted by 15 U.S.C. § 1681t(b)(1)(F)); *Jaramillo v. Experian Info. Sols., Inc.*, 155 F. Supp. 2d 356, 361-62 (E.D. Pa. 2001) (concluding that claim under the Pennsylvania Unfair Trade Practices and Consumer Protection Law based on underlying violation of the FCRA was preempted by 15 U.S.C. § 1681t(b)(1)(F)).

program detects and responds" to various types of activity that NYAG considers to constitute Red Flags, such as wire requests occurring shortly after password changes. (Compl. ¶ 315 (emphasis added).) NYAG's expansive theory greatly misconstrues the Red Flags Rule, which requires only that a covered bank "***develop and implement*** a written Identity Theft Prevention Program (Program) that is ***designed*** to detect, prevent, and mitigate identity theft . . . ." 12 C.F.R. § 41.90(d) (emphasis added).

On its face, the Complaint does not allege a violation of the Red Flags Rule. NYAG nowhere alleges that Citibank failed to adopt a written policy, nor does it allege that there are any particular faults with any policy's terms. The Complaint even fails to allege the steps that Citibank took to determine that the wires of Consumers A through J should go forward, making it impossible to infer anything about Citibank's written policies and why they are allegedly inadequate. That, according to the Complaint, sophisticated scammers have in some instances found ways to commit fraud simply does not make out a violation of the Red Flags Rule, much less show "persistent" or "repeated" illegality under Executive Law § 63(12).

Importantly, and contrary to NYAG's suggestion, the Red Flags Rule does not obligate a bank to freeze a transaction in the presence of a Red Flag. There is no requirement, for example, to deny all wires on the same day as a password change, or where the wire amount involves most or all of the funds available. Even assuming those situations count as Red Flags (which they may not), Citibank's obligation under the Red Flags Rule would be, at most, to have a policy "designed" to identify when those things occur and to respond. Yet NYAG's Complaint alleges nothing about what Citibank's identity theft policies are with respect to these or any other purported Red Flags.

NYAG is not the first litigant to try (and fail) to impose strict liability under regulations that require only the development, implementation and administration of policies and procedures, similar to the Red Flags Rule. Courts have been careful to heed the difference.

For example, in *Smith v. Franklin/Templeton Distributors, Inc.*, No. C 09–4775 PJH, 2010 WL 4286326 (N.D. Cal. Oct. 22, 2010), an investor accused an investment fund of improperly engaging unregistered broker-dealers, in violation of an SEC regulation requiring that funds "[a]dopt and implement written policies and procedures reasonably designed to prevent violation of the Federal Securities Laws." 17 C.F.R. § 270.38a-1(a)(1); 2010 WL 4286326, at *3. The court dismissed the claim, observing that the regulation "simply requires funds to adopt and implement compliance programs that are reasonably designed to prevent violation of the federal securities law," and the investor had alleged nothing about the fund's policies. *Id*.

Similarly, in *Mastin v. Ditech Financial, LLC*, No. 3:17cv368, 2018 WL 524871 (E.D. Va. Jan. 23, 2018), a couple accused their mortgage servicer of violating a regulation requiring it to "maintain policies and procedures that are reasonably designed to" provide borrowers with information and to investigate their complaints. *Id*. at *6; 12 C.F.R. § 1024.38(a). Dismissing the claim, the court observed that the regulation "requires 'only that a lender enact policies' that effectuate the goals outlined," whereas the couple only alleged "isolated instances where [the] procedures may have been deficient." 2018 WL 524871, at *6 (citation omitted).[14]

[14] *See also*, *e.g.*, *Mikel v. Carrington Mortg. Servs., LLC*, A-16-CV-1107, 2019 WL 4060890, at *7 (W.D. Tex. June 25, 2019) (dismissing homeowner's claim that bank violated requirement in 12 C.F.R. § 1024.40's that lenders "maintain policies and procedures that are reasonably designed to" make their personnel available to borrowers, because plaintiffs had "come forward with no evidence regarding [the servicer's] policies and procedures"); *Hines v. Regions Bank*, No.: 5:16-cv-01996, 2018 WL 905364, at *5 (N.D. Ala. Feb. 15, 2018) (dismissing similar claim, arising from servicer allegedly having "consistently ignored" plaintiff's calls, because plaintiff did "not allege that [bank] failed to implement policies reasonably designed to achieve [the regulation's] objectives," but had alleged "only that [the bank] did not achieve those objectives in handling his mortgage delinquency"); *accord Little Rock School Dist. v. Armstrong*, 359 F.3d 957, 965 (8th Cir. 2004) (explaining that consent decree provision requiring that school district "implement" certain programs "does not mean that the programs must be perfectly efficacious").

Here, because NYAG does not adequately allege that Citibank failed to adopt a policy as required by the Red Flags Rule, NYAG has not pleaded any illegality (nor any "repeated" illegality) under Executive Law § 63(12). The Sixth Cause of Action should be dismissed.

VI. The Fifth Cause of Action Based on the SHIELD Act Should Be Dismissed.

NYAG's claim based on New York's SHIELD Act is similarly meritless because (1) it deals with an entirely different subject matter than the unauthorized wires at issue in this case, (2) NYAG has not pleaded facts showing that Citibank failed to implement an anti-hacking policy, and (3) in the alternative, to the extent the SHIELD Act is read as NYAG proposes to cover a bank's antifraud procedures, it is preempted by the FCRA.

A. New York Adopted the SHIELD Act to Combat Hacks and Data Breaches.

The SHIELD Act (which stands for the Stop Hacks and Improve Electronic Data Security Act) was enacted in 2019 to update New York's prior data breach notification law so as to "require reasonable data security protections" for covered businesses and to "update[] the notification procedures" for "when there has been a breach of private information." N.Y. Bill Jacket, L. 2019, Ch. 117, at 7-8. The SHIELD Act is focused on preventing and remedying hacking and data breaches, which is why covered entities must, for example, have a security system that "assesses risks in network and software design" and "detects, prevents and responds to attacks or system failures." N.Y. Gen. Bus. L. § 899-bb(2)(b)(ii)(B). When those "attacks" succeed, or there is a data breach, covered businesses are required to notify the affected customers "in the most expedient time possible and without unreasonable delay." *Id.* § 899-aa(2).

NYAG has enforced these provisions against, for example, a law firm hit with a ransomware attack that exposed extensive sensitive information concerning hospital clients (*see* Ex. Q) and a dental insurer that fell for a "phishing" scam that gave the attackers access to extensive data about its policyholders (such as Social Security numbers) (*see* Ex. R).

B. The SHIELD Act's Anti-Hacking and Customer Notice Provisions Are Inapplicable.

Straying far beyond the text and purpose of the SHIELD Act, NYAG alleges that Citibank has violated the Act by failing to stop wires in the face of "anomalous account activity," such as when wires are sent after password changes or enrollments in a wire transfer service, or when wires are in amounts that would leave the account with a "near-zero" balance. (Compl. ¶ 305.) But the SHIELD Act does not actually address whether and under what circumstances banks should approve wires. Rather, it is a law focused on hacking and data breaches, not wires initiated by fraudsters who exploited data gained elsewhere, often directly from the customer. Indeed, the Complaint nowhere alleges that fraudsters hacked into Citibank's systems. For example:

- Consumer C's data was compromised because of a "security incident" at a "mortgage servicing firm" holding his loan. (*Id.* ¶ 154.)
- Consumers E and G were victims of a "SIM swap" scam, whereby the subscriber identity module (or, SIM) of their phones was reassigned to a fraudster's mobile device. (*Id.* ¶¶ 169-70, 198-99, 206.)
- Consumers F and I provided fraudsters their personal data over the internet. (*Id.* ¶¶ 183-84, 234.)
- Consumers H and J provided fraudsters their personal data over the phone. (*Id.* ¶¶ 218-19, 249-50.)

NYAG should not be permitted to stretch the SHIELD Act, beyond its stated purpose and plain language, into a regulation-by-litigation of which wire requests should be accepted.

C. NYAG Fails to Allege Facts Showing a SHIELD Act Violation.

In addition to the SHIELD Act not being implicated, there is yet a further, independent ground for dismissal. Like the Red Flags Rule, the SHIELD Act is limited in scope, requiring only that covered businesses "implement[] a data security program that includes" certain "reasonable . . . safeguards." N.Y. Gen. Bus. L. § 899-bb(2). The Complaint does not allege that

Citibank failed to implement a program with reasonable safeguards or, in fact, anything about the program that Citibank has implemented. As discussed above with respect to the Red Flags Rule (*see* § V.C), merely alleging that scammers succeeded in certain instances does not show a violation of the SHIELD Act, particularly absent factual allegations as to whether the scammers were able to do so in a manner within the Act's scope.

D. Alternatively, the FCRA Preempts NYAG's SHIELD Act Claim.

As discussed above, the FCRA broadly preempts any state-imposed "requirement or prohibition . . . with respect to the conduct required by" the Red Flags Rule. 15 U.S.C. § 1681t(b)(5)(F). Here, if the SHIELD Act is read to extend to the conduct about which NYAG complains, then it impermissibly overlaps with the "conduct" covered by the Red Flags Rule, and, as in *Willey* and *Elias*, is preempted. The Complaint itself makes the overlap clear; NYAG alleges that Citibank's violations of the SHIELD Act arise from the ***same*** alleged failures to act upon the ***same*** alleged anomalous activity as with the Red Flags Rule, such as approving wires after password changes. (*Compare* Compl. ¶ 305 *with id*. ¶ 315.) Therefore, if the SHIELD Act is as broad as NYAG suggests, the FCRA preempts NYAG's state-law claim.

VII. The Seventh and Eighth Causes of Action Should Both Be Dismissed Because NYAG Pleads No Facts Showing Fraud Under Executive Law Section 63(12) or Deception Under General Business Law Section 349.

In a seeming afterthought, NYAG's final two claims allege that Citibank handles online fraud in a manner that is not just incorrect, but fraudulent under Executive Law § 63(12) (Seventh Cause of Action) and deceptive under General Business Law § 349 (Eighth Cause of Action). These claims are an overreach and wholly unsupported by the allegations.

As discussed, to plead a claim under Executive Law § 63(12), NYAG must allege that Citibank "engaged in 'repeated' fraudulent or illegal acts" or "engaged in 'persistent fraud or illegality'" in "carrying on, conducting, or transacting a business." *People of the State of New*

York v. Wu, No. 452904/2022, 2024 WL 776820, at *10 (N.Y. Sup. Ct. Feb. 26, 2024). The elements of a claim under General Business Law § 349 are similar, but also include an injury component: NYAG must allege that Citibank engaged in an "act or practice that is deceptive or misleading in a material way and that the consumer has been injured by reason thereof." *People ex rel. Spitzer v. Applied Card Sys.*, 834 N.Y.S.2d 558, 562 (3d Dep't 2007) (alteration omitted).

For purposes of General Business Law § 349, it is not enough to assert that an act or practice is deceptive; the complaint must allege "what facts, if any, support" that conclusion. *Wiggins v. Unilever U.S., Inc.*, No. 21 Civ. 1964, 2023 WL 7005147, at *15 (S.D.N.Y. July 26, 2023). New York courts "routinely dismiss" Section 349 claims "where the allegations are insufficiently specific to establish a deceptive practice." *Canestaro v. Raymour & Flanigan Furniture Co.*, No. 2012-1639, 2013 WL 6985415, at *2 (N.Y. Sup. Ct. May 20, 2013).

For both claims, NYAG sets forth an identical set of allegations that can be grouped into three categories: (1) statements Citibank made concerning account security; (2) Citibank's requests for affidavits of fraud; and (3) Citibank's supposed violations of customers' "rights and obligations." (Compl. ¶¶ 319(a)-(h), 324(a)-(h).) The allegations in each category fall short.

A. Citibank's Statements About Account Security Are Not Actionable.

NYAG alleges that Citibank misled its customers by "creating the impression that online and mobile banking were no less secure than in-person banking." (Compl. ¶¶ 319(a), 324(a).) There is no indication, however, as to how this "impression" was created, nor any allegation that Citibank ever suggested the two were the same.

The Complaint similarly accuses Citibank of falsely "having represented that bank accounts were secure" (*id.* ¶¶ 319(c), 324(c)), by virtue of advertisements with generic statements like, "As always at Citi, your security is important to us" and "We, at Citi, consider your security to be the topmost priority." (*Id.* ¶ 83.) But these statements amount to non-

actionable "puffery" rather than factual claims that could deceive. *See DH Cattle Holdings Co. v. Smith*, 607 N.Y.S.2d 227, 231 (1st Dep't 1994) (statement about a "safe investment" was "mere opinion and puffery"); *Tristan v. Bank of Am.*, No. SACV2201183, 2023 WL 4417271, at *4-5 (C.D. Cal. June 28, 2023) (no fraud based on allegations that payment service Zelle was represented to be "simple," "fast," and "safe").

Common sense and case law confirm that aspirational language like this is not actionable. For example, a reference in a hospital system's "Patients' Bill of Rights" to safeguarding patient data does "not constitute an unlimited guaranty that patient information could not be stolen or that computerized data could not be hacked." *Abdale v. N. Shore-Long Is. Jewish Health Sys.*, 49 Misc. 3d 1027, 1032, 1039 (N.Y. Sup. Ct. 2015). Nor does a medical practice advertising "we have the solution" amount to a "guarantee of results" or assurance that there are "no risks" involved in surgery. *Corcino v. Filstein*, 820 N.Y.S.2d 220, 221 (1st Dep't 2006).

There is no allegation that any of Consumers A through J ever saw, much less were harmed by, any alleged misrepresentations. Thus, NYAG's claims about Citibank's statements concerning online security should be dismissed.

B. Citibank's Requests for Fraud Affidavits Neither Deceived nor Injured Any Consumer.

NYAG next complains that Citibank's response to customer complaints was fraudulent and deceptive because Citibank required customers to execute affidavits concerning the circumstances of the fraud they were reporting. (Compl. ¶¶ 319(d)-(f), 324(d)-(f).) Apparently, NYAG disagrees with the practice of requiring online fraud victims to set forth what happened in affidavit form. But NYAG's dislike of the practice does not make it deceptive or materially misleading. In *Cline v. TouchTunes Music Corporation*, 211 F. Supp. 3d 628, 635-36 (S.D.N.Y. 2016), for example, users of an online music service complained that the service refused "to

refund credits for unplayed songs." *Id.* at 635-36. Judge Kaplan rejected the claim because the users had "not alleged any facts to suggest that they reasonably expected such a refund," explaining that "[t]he mere fact that plaintiffs find this particular business practice distasteful does not make it deceptive or misleading." *Id*. So too here.[15]

NYAG also fails to allege (nor could it credibly allege) how any consumer was injured as a result of the affidavit requirement. *See Polzer v. TRW, Inc.*, 682 N.Y.S.2d 194, 195 (1st Dep't 1998) (§ 349 does not compensate for "frustration," and dismissing claim because plaintiff was not damaged by allegedly deceptive conduct). To the extent NYAG complains that Citibank used information in the affidavit to deny consumer's refund requests, there is no plausible suggestion of injury, since the information would have been gathered in one form or another to evaluate the customer's claim of fraud.

C. Citibank's Alleged Violations of the "Rights and Obligations" of Customers Are Neither Fraudulent Nor Deceptive.

Finally, NYAG claims that Citibank violated the "rights and obligations" of customers by "failing to immediately investigate" issues, by "having not immediately attempted to recall funds," and by telling customers "they acted improperly," so as to "deprive[] them of their legal rights to recover stolen funds." (Compl. ¶¶ 319(b), (g), (h), 324(b), (g), (h).) These allegations do not even purport to describe deceptive conduct.

Nor does NYAG plead fraud by alleging consumers were misled into "believ[ing] that their own actions were relevant" to determining whether they would be reimbursed (*id*.

---

[15] *See also*, *e.g.*, *Varela v. Investors Ins. Holding Corp.*, 615 N.E.2d 218, 219 (N.Y. 1993) (holding that law firm's refusal to file a satisfaction of judgment until judgment debtor paid it a fee, while potentially improper, was not deceptive under § 349); *Leider v. Ralfe*, 387 F. Supp. 2d 283, 296 (S.D.N.Y. 2005) (holding that alleged "monopolistic practices" did not make out a § 349 claim because they were "public knowledge"); *Sands v. Ticketmaster-New York, Inc.*, No. 31614/92, 1994 WL 662956, at *2 (N.Y. Sup. Ct. June 23, 1994) (rejecting § 349 claim about "the manner in which Ticketmaster computes its service charges," noting that because Ticketmaster "fully discloses the service charges," "the manner of their computation is not a deception that violates § 349").

¶ 319(h)), given that customers' actions obviously ***are*** relevant to the analysis. If a fraudster was able to satisfy the relevant security procedures for an outbound wire because the customer provided the fraudster with the tools to do so, then that fact bears on Citibank's reimbursement obligations under N.Y. U.C.C. § 4-A-202(2).

Even assuming the EFTA were to apply (which it does not), the circumstances of the transfer would likewise be relevant. Under the EFTA, a transfer is not considered unauthorized if "initiated by a person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer." 15 U.S.C. § 1693a(12); *see, e.g.*, *Merisier v. Bank of Am., N.A.*, 688 F.3d 1203, 1210 (11th Cir. 2012) (holding that bank was not liable for withdrawals where account holder "furnished the means of access to her account voluntarily, either as a willing participant in a fraudulent scheme or as one duped" by the fraudsters). Citibank would need to know (among other things) whether or not that provision was triggered. In alleging that customer's "own actions" are categorically not relevant, NYAG appears to be suggesting that Citibank is obligated to refund ***every*** claim of wire fraud, without ***any*** investigation as to what happened. That simply is not the law.

At bottom, disagreement over the law that should govern Citibank's investigative process does not mean Citibank's actions can be shoehorned into claims of fraud or deception. NYAG's claim for fraud under Executive Law § 63(12) and its consumer deception claims under General Business Law § 349 should be dismissed.

CONCLUSION

For the stated reasons, the Court should grant Citibank's motion to dismiss in its entirety.

Dated: April 2, 2024

Respectfully submitted,

STEPTOE LLP

By: */s/ Charles Michael*

James L. Brochin
Charles Michael
Meghan Newcomer
1114 Avenue of the Americas
New York, New York 10036
(212) 506-3900
jbrochin@steptoe.com
cmichael@steptoe.com
mnewcomer@steptoe.com

Julia Strickland*
David Moon*
2029 Century Park East
Suite 1800
Los Angeles, CA 90067
(213) 439 9400
jstrickland@steptoe.com
dmoon@steptoe.com

* *pro hac vice* application forthcoming

Counsel for Citibank N.A.